Mapping of Industrial Assets FAQs

Briefing Call held on Tuesday 26th September 2023

Question 1:
How should we approach the use of AI? Is standardization of data models key? Should there be transferrable standardization of the data model across your domain?
Answer 1:
Data models, AI, and this is very much a stretch goal and not a core part of the requirement. Any data model you use would be under your decision to use as part of the challenge.

There are no constraints on the data models or standards.

Discussion:
We (collaborator) work in the digital twin space, is this part of the cyber physical infrastructure strategy that the UK Government have been setting out, so is their preference to look at open standards.

We (Collaborator) work with the Open Connectivity Foundation, which meets the majority of all security baselines for communications.

The primary aim here is to do something like derived metrics which are true and known, and then if you wanted to use AI, that would be purely to enhance the granularity of information or the detail there.
The data model question really comes down to what ability you have to generate data or to start to look at that. On the second point on the Open Connectivity Foundation, more than happy for open standards to be considered as part of your discovery work as long as you're considering how they might integrate into existing network of legacy technologies.

We want to see a consideration of wide gamut of technologies, not just sort of a single standard, so the ability to do asset discovery across varying and different distributed systems that has lots of different technologies.

We recognise those concerns around building models based on perceptions and bias and that sort of piece, so really would encourage a proposal that includes how we might mitigate those things.

Question 2:
Can you provide an example of what assets you were looking at?
Answer 2:
We're looking at quite a wide range, so keen for it to cover everything with the system, but with a primary focus on some of the more neglected assets like remote terminal units, programmable logic controllers, gateways for digital pumps, scada gateways.

Discussion:
If you're familiar with the Lower Level Purdue model, zero layer one devices and then expanding up from there, but with a particularly focus here on run assets, which could be any

programmable logic controllers or similar units like HMIS would be some of the key ones, but the list does go beyond them.

Question 3:
From a digital twin perspective do you have defined processes that exist already that monito these assets and have some form of feedback loop to monitor its efficiency?
Answer 3:
For the purpose of this challenge assume we don't have any existing defined processes for doing this.

Question 4:
In terms of secure mesh networks, what is the potential coverage needed, also in terms of chip designs for the gateway, are there any restrictions? Would you also want to track the hardware and software bill of materials?
Answer 4:
There are no restrictions on chip designs for the gateway, tracking hardware or software bill of materials would also be desirable.

Question 5:
Is there a proposals format to us to follow?
Answer 5:
We would like more than just theory; it would be good to see a concept demonstrator or a proof of concept.

Question 6:
Are there any restriction on the communication methods used? Are you looking at fixed assets on a fixed network or RF communication methods? OK, to do remote detection etc.?
Answer 6:
RF methods and those similar are encouraged, that includes links in potential black spots. So if you have a proposal that involves the ability to either do asset monitoring across the existing roof links or LoRaWAN technologies or anything on those lines, that's definitely interesting.

Discussion:
Equally interesting to be able to identify when traffic is entering gateways and you believe it would not be able to be detected due to data flooding at the gateway.

We (National Security) use LoRaWAN a lot, potentially within smart cities or within smart factories primarily for sensor networks

Moving out to the bigger picture we use LoRaWAN for our remote IT sensors, deployment, cities etc.

Question 6:
Are you looking for a strategic map of the location of these devices or just identification of what devices are on the LoRaWAN network? I'm just trying to work out what you're trying

to get other than what you can get from an existing cloud service that that you'd run over the top.

Answer 6:
With LoRaWAN, one option is you just take it off that gateway, but making sure that's aggregated into the other information you're generating off the wider estate.
If you are able to pull that data off a gateway or off your cloud service, then you should be looking to do that rather than sending lots of traffic down your LoRaWAN link.

If you've got anything hanging off a LoRaWAN device, then you want to make sure that's noted.
Look to using things like LoRaWAN gateways that have existing sensors and aggregation, leveraging the capabilities of existing technologies within a network with new sensor nodes.

Question 7:
Most serial to IP converters and protocol converters are silent, just changing the electrical properties from one protocol to the other, are you looking to make those a bit more intelligent so they're discoverable?

Answer 7:
Yes, that is one approach you could take. The other approach would be looking at common protocols that you know might be converted, for example something like modbus RTU as a random example of industrial control.
You know that can be run over modbus TCP as well as a modbus TCP connection and might be converted into modbus RTU and run over a serial link. It's potentially looking at how you can use novel ways of doing it.
How you can look at that traffic and identify a modbus TCP.
Am I seeing the end to end connection or does that look like it might be being converted and going down serially somewhere else?
Or equally, am I sending TCP encapsulated or slip encapsulated serial data across my network?
In which case, how do I truly know?
Well, that's ending up and making sure that those kind of nuances are highlighted within an asset discovery method so that the operator is informed to be able to carry out their manual assessments after the automated solution.
Does that make sense?

Discussion:
The ultimate goal is to understand all the assets in the chain, so you can look at the vulnerabilities that you might have.

The challenge is that a lot of companies don't truly understand what assets they have.
You could look at firmware versions across the estate of assets.
First steps here is really just working out exactly what is in the estate and when that's changing.

If you've got 15,000 of these assets distributed across thousands of sites, it's surprisingly easy to lose track of exactly what you have at each site, so it's really just trying to work out the complete picture.
Extra information could be added on top such as firmware versions which indicate the kind of published vulnerability that might exist.

Question 8:
How much coverage is needed?

Answer 8:
As much as possible of the full system

Discussion:
You can obviously create a more well defined secure mesh network within a smaller environment.
So I'm thinking here, with the likes of LoRaWAN, when you've got a huge coverage area, but in terms of your asset monitoring, these are likely to be well defined in smaller areas, for example we have a very highly secure RF chip design that will be utilized within our gateways, but the coverage is limited to small areas.
We are thinking about the assets and the hardware, the limitations and the software bill of materials within a digital twin concept.
You know where potential vulnerabilities could exist so that you can track and monitor those assets using data.
I think it will definitely be interesting to see a proposal on it and I would welcome you to include that within your proposal.